(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－167553

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ ３３０Ｂ

審査請求　未請求　請求項の数２　ＯＬ　（全　４　頁）

(21)出願番号　特願平9－331494

(22)出願日　平成９年(1997)12月２日

(71)出願人　597168402
成山　吉明
大阪府豊中市中桜塚３－３－17　サンロイヤル中桜塚503

(72)発明者　成山　吉明
大阪府豊中市中桜塚３－３－17　サンロイヤル中桜塚503

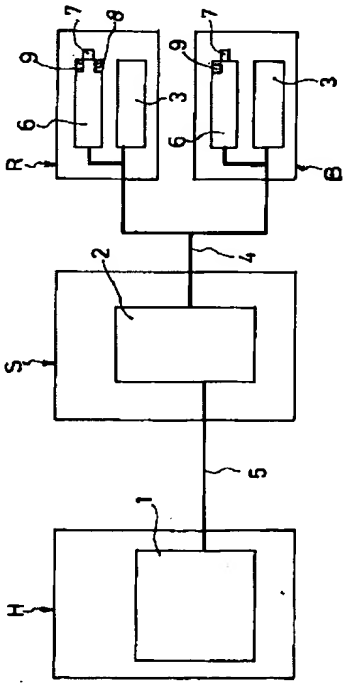
(74)代理人　弁理士　北谷　寿一

(54)【発明の名称】　オンラインシステムでの本人確認システム

(57)【要約】

【課題】　高いセキュリティの下で、真にサービスを利用し得る資格者本人たることを確認でき、第三者の不正利用による財産上の損失等を未然に防止できるオンラインシステムでの本人確認システムを提供する。

【解決手段】　ホストコンピュータ(２)と、入力手段を有する端末装置(３)とを通信回線(４)で連結接続する。ホストコンピュータ(２)に記憶されている個人情報に関連づけてパスワードを記憶させる。個人識別情報を前記パスワードと関連づけて記憶させている第２コンピュータ(１)をホストコンピュータ(２)に接続する。端末装置(３)からホストコンピュータ(１)にアクセスした際に、パスワードとともに個人識別情報を端末装置(３)の入力手段から入力し、第２コンピュータ(１)に記憶されている個人識別情報と入力された個人識別情報とを照合する。その照合による合致率を第２コンピュータ(１)からホストコンピュータ(２)に伝達する。



1

【特許請求の範囲】

【請求項１】　個人情報を記憶しているホストコンピュータ(２)と、入力手段を有す端末装置(３)とを通信回線(４)で連結接続してなるオンラインシステムにおいて、ホストコンピュータ(２)に記憶されている個人情報に関連づけてパスワードを記憶させ、個人識別情報を前記パスワードと関連づけて記憶させている第２コンピュータ(１)をホストコンピュータ(２)に接続し、端末装置(３)からホストコンピュータ(１)にアクセスした際に、パスワードとともに個人識別情報を端末装置(３)の入力手段から入力し、第２コンピュータ(１)に記憶されている個人識別情報と入力された個人識別情報とを照合し、その照合による合致率を第２コンピュータ(１)からホストコンピュータ(２)に伝達するようにしたオンラインシステムでの本人確認システム。

【請求項２】　個人識別情報が網膜パターンや虹彩の模様等の眼球情報、指紋や声紋等の個人身体的特徴情報、筆跡や筆圧等の個人特有の癖情報から選ばれたの少なくとも１種類であるオンラインシステムでの本人確認システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クレジットカードや電子マネーの利用等そのサービスを利用する際に会員資格等の一定の資格が求められる場合に、資格者本人たることを確認して第三者の不正な利用を効果的にカットできるオンラインシステムでの本人確認システムに関する。

【０００２】

【従来の技術】従来、クレジットカードの利用者は、自己のカードを加盟店等に提示してサイン等をすることにより一定限度内の買物をしたり、融資を受けたりできるようになっている。

【０００３】

【発明が解決しようとする課題】しかし、カードが真正なら、たとえ本人でなくても利用できてしまう問題があり、紛失・盗難等によりカードを無断使用された会員が損害を被る問題がある。又、カードが偽造され、カードチェッカーをクリアしてしまえば、不法者の利用をそのまま許してしまう問題もあり、架空名義のカードによりクレジットカード会社等が損害を被る問題もある。

【０００４】これらの防止策として、入会時、更新時等にカードに本人の顔写真を入れる提案があるが、写真を撮られたり、常時カードに自分の写真が付帯することについて抵抗感を覚える人が少なくないし、又、写真入りだと逆に持ち主がすぐに誰だかわかって、その者をねらい打ちにした悪用を助長する懸念もある。

【０００５】又、クレジットカードとは別に、指紋情報をデジタル化して本人確認用ＬＳＩカードに記録し、サービスの利用時にこのＬＳＩカードと本人の指とを照合

2

する提案もされている。しかしながら、カードを常時２枚携帯して運用する煩雑さがあるし、仮にクレジットカードとＬＳＩカードとを１本化したとしても、常時ユーザーの末端において外部と接するカード自体に個人情報を付帯させているという点で、偽造の懸念が払拭できず、偽造団とのいたちごっこは不可避的であって、セキュリティを保証し難い致命的欠点がある。

【０００６】本発明の主目的は、高いセキュリティの下で、真にサービスを利用し得る資格者本人たることを確認でき、第三者の不正利用による財産上の損失等を未然に防止できるオンラインシステムでの本人確認システムを提供する点にある。

【０００７】

【課題を解決するための手段】上述の目的を達成するために本発明は、ホストコンピュータに記憶されている個人情報に関連づけてパスワードを記憶させ、このパスワードと関連づけて個人識別情報を記憶させている第２コンピュータをホストコンピュータに接続し、端末装置からホストコンピュータにアクセスした際に、パスワードとともに個人識別情報を入力手段から入力し、第２コンピュータに記憶されている個人識別情報と入力しされた個人識別情報とを照合し、その照合による合致率を第２コンピュータからホストコンピュータに伝達するようにしたことを特徴としている。

【０００８】ここで、個人識別情報は、人の目の眼球壁の最内層たる網膜の血管パターン（網膜パターン）や、虹彩の模様等の眼球情報の他、指紋、声紋、筆跡等の個人によって異なる固有の情報を含む概念である。また、入力手段での入力とは、クレジットカードの提示や、これに引き続くカードの読取、或は、キーボードからのパスワードの手入力、申込書類への必要事項の記入、会員番号や氏名等の口答申告といった行為を含む概念である。

【０００９】また、個人情報とは、顧客番号、氏名、生年月日、性別、住所、電話番号、職業、財産情報等を広範囲に含む概念であり、パスワードとは予め登録されている文字や記号あるいは数字の組み合わせによる数桁の文字列で構成されたものをいう。

【００１０】

【発明の作用】本発明では、ホストコンピュータに個人情報をパスワードと関連ずけて登録(記憶)するとともに、ホストコンピュータに情報伝達可能に接続されている第２コンピュータに各人の個人識別情報を前記パスワードと関連づけて登録(記憶)しておく。

【００１１】次いで、各加盟店等でサービスを利用する場合は、端末装置の入力手段からパスワードとともに個人識別情報を入力する。この入力する信号情報は通信回線を介してホストコンピュータにアクセスし、個人情報のファイルが開かれるとともに、パスワードと個人識別情報が第２コンピュータに伝送される。そして、第２コ

ンピュータで入力された個人識別情報と予め登録されている個人識別情報とを照合し、既登録個人識別情報と入力された個人識別情報の合致率をホストコンピュータに伝送する。

【００１２】既登録個人識別情報が無い場合には合致率は当然０となるし、他人カードなどが使用された場合では入力されたパスワードに対応する既登録個人識別情報は存在するが入力にかかる個人識別情報と合致しないことから、この場合にも合致率は０あるいは極めて低い値となる。一方、正規のカード保有者が利用する場合には、既登録個人識別情報と入力個人識別情報は基本的には完全に合致するはずであるが、体調やそのときの入力方法等により、完全合致までは至らなくても、この場合には、高い合致率を示す。

【００１３】そこで、合致率をホストコンピュータ側に送り、ホストコンピュータ側で定めた合致率以上の場合に本人であると確認するようにしてなっている。したがって、定められた合致率に至らない場合には、ホストコンピュータ側からサービス提供の拒絶指令を出すことにより、不正者の利用を排除することができる。そして、個人識別情報は末端に開放されることがないから、偽造の心配はなく、高いセキュリティを確保することができることになる。

【００１４】

【発明の実施の形態】図１において、符号(１)は本人確認システムの中核を担う本人確認会社等の本人確認機関（以下、確認機関Ｈという）に設置した第２コンピュータ、(２)はクレジットカード会社等のサービス提供機関（以下、サービス機関Ｓという）に設置したホストコンピュータ、(３)は加盟店等の複数あるサービス利用機関（以下、利用機関Ｒという）やカード会員の登録を受付ける銀行等の複数ある登録機関（以下、登録機関Ｂという）に設置した端末装置であり、ホストコンピュータ(２)と端末装置(３)、及びホストコンピュータ(２)と第２コンピュータ(１)とはそれぞれ通信回線(４)(５)で接続している。

【００１５】サービス機関Ｓのホストコンピュータ(２)には、顧客番号、氏名、生年月日、性別、住所、電話番号、職業、財産情報等の個人情報がパスワードと関連づけて記憶させてある。

【００１６】登録機関Ｂには、個人識別情報たる網膜パターンを読取る網膜パターン読取機(６)が設置している。その登録は、入会者がファインダー(７)を左右何れかの片目で覗きながら登録キー(８)を作動させることにより起動される。そして、確認会社Ｈにおいて、網膜パターン読取機(６)と連携するソフトウェア資源から成る個人情報登録手段により、第２コンピュータ(１)の管理ファイル上に、その読取った網膜パターンのディジタル情報が個人識別情報としてパスワードと共に登録される。従ってこの場合網膜パターン読取機(６)が端末装置(３)の一部を構成している。

【００１７】登録機関Ｂの網膜パターン読取機(６)は登録だけでなく、既登録パターンとの照合も行えるようになっており、ファインダー(７)を片目で覗きながら照合キー(９)を作動させることにより、読み取った網膜パターンのデジタル情報がホストコンピュータ(２)を介して確認機関Ｈの第２コンピュータ(１)に伝送されるようにしてある。従って登録機関Ｂの端末装置(３)の操作によりサービス機関Ｓからのサービスが受けられるようになっている。

【００１８】利用機関Ｒには、カードリーダやキーボードあるいはタッチパネル等の入力手段と、登録機能を保有しない網膜パターン読取機(６)が配置してあり、前記と同様ファインダー(７)を片目で覗きながら照合キー(９)を作動させることにより、読み取った網膜パターンのデジタル情報がホストコンピュータ(２)を介して確認機関Ｈの第２コンピュータ(１)に伝送されるようにしてある。この場合には、入力手段と網膜パターン読取機(６)が端末装置(３)を構成している。

【００１９】そして、利用機関Ｒや登録機関Ｂからサービス機関Ｓにアクセスする際には、キャッシュカードやクレジットカード等のカード類が使用されるが、このカード類にはカード番号等のカード情報が記録されている。このカード情報は生のデータとして記録してあってもよいが、暗号化処理したデータであってもよい。またカードとしては情報を磁気テープに記録したものでも、情報を記録したＩＣチップを埋め込んだものであってもよい。

【００２０】利用機関Ｒや登録機関Ｂからサービス機関Ｓにアクセスする場合には、入力手段に挿入したカード類のデータとパスワードとがサービス機関Ｓのホストコンピュータ(２)に伝送され、ホストコンピュータ(２)に記録されている個人情報ファイルと照合される。ここでカード類に記録されているデータに対応している登録パスワードと入力パスワードが不一致の場合には、無資格者と判断して、以後のサービス付与が停止される。

【００２１】一方、カード類に記録されているデータに対応している記録パスワードと入力パスワードが一致した場合には、利用機関Ｒ等の端末機器に個人識別情報(網膜パターン)の入力を促し、入力された網膜パターンをデジタル処理して確認機関Ｈの第２コンピュータ(１)にサービス機関Ｓのホストコンピュータ(２)を介して伝送される。確認機関Ｈの第２コンピュータ(１)に伝送された網膜パターンのデジタル情報は、第２コンピュータ(１)に予め登録されている網膜パターンのディジタル情報と照合され、第２コンピュータ(１)でその合致率を算出する。なお、この照合作業は、サービスを受ける者がホストコンピュータ(２)にアクセスした際のパスワードをキーとして、入力パスワードをホストコンピュータ(２)から第２コンピュータ(１)に伝達し、第２コンピュ

ータ(１)で予めそのパスワードに対応する登録個人識別情報を抽出しておくことにより、短時間に行うことができる。

【００２２】確認機関Ｈの第２コンピュータ(１)で算出された合致率は、サービス機関Ｓのホストコンピュータ(２)に伝達される。ここで、合致率は、覗き込む目の角度、姿勢等によって照合のたびに変動することから、最も近似した既登録パターンとの合致率を算出合致率としている。第２コンピュータ(１)からホストコンピュータ(２)に伝達された合致率が、サービス機関Ｓにおいて予め設定している基準値(例えば７０％)以上である場合にホストコンピュータ(２)が同一人であると判定しサービスの付与を行うようにしている。

【００２３】尚、合致率の基準値を如何に定めるかは、結局、誤認率をどの程度許容するかによる。因に７０％であれば、数１０万回～１００万回に１回程度の誤認率に収まり、実使用上問題はない。もっとも、この数値よりも高い値、低い値を選定しても勿論よい。

【００２４】上述の実施形態では、確認機関Ｈではサービス利用者が資格者本人たることの確認のみをするものとし、いわゆるブラックリストに載っているか否かは判断しないで、このような財産上の不良な会員の排除は、サービス機関Ｓに委ねる仕様にしている。確認機関Ｈによる独自のサービスは本人確認のみに止まるが、個人のプライベートデータの管理を現状通りサービス機関Ｓにそのまま集中保持させておくことができるメリットがある。

【００２５】尚、網膜パターン読取機(６)はサービス機関Ｓに設置し、サービス機関Ｓ自体で会員登録できるものとしても勿論よい。さらに網膜パターン読取機(６)を、特に信頼の厚い利用機関Ｒに設置してもよい。この場合、登録時と利用時の読取機を一つのものに統合できる。

【００２６】上記の実施態様では、個人識別情報として網膜パターンを使用するものに付いて説明したが、個人識別情報としては、虹彩模様、指紋、声紋等の個人特有の身体的特徴や筆圧や筆跡等の個人固有の癖を利用したものを使用するものであってもよい。

【００２７】

【発明の効果】本発明では、従来からオンラインシステムで使用されているカードやパスワードに加えて各個人特有の特徴である身体的特徴情報や癖情報等の個人識別情報を使用して本人確認を行うようにしているので、予め登録されている者以外の利用を排除することができ、高いセキュリティを維持することができる。

【図面の簡単な説明】

【図１】本発明に係る本人確認システムの第１実施形態の構成図。

【符号の説明】

１…第２コンピュータ、２…ホストコンピュータ、３…端末装置、４・５…通信回線。

【図１】